



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/755,470	01/05/2001	Steven Branigan		4994

27997 7590 12/29/2005

PRIEST & GOLDSTEIN PLLC  
5015 SOUTHPARK DRIVE  
SUITE 230  
DURHAM, NC 27713-7736

EXAMINER
----------

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 12/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Advisory Action  
Before the Filing of an Appeal Brief**

Application No.

09/755,470

Applicant(s)

BRANIGAN ET AL.

Examiner

Ellen C. Tran

Art Unit

2134

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 30 November 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☐ The period for reply expires \_\_\_\_\_ months from the mailing date of the final rejection.  
b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on \_\_\_\_\_. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because  
(a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);  
(b) ☐ They raise the issue of new matter (see NOTE below);  
(c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or  
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: See Continuation Sheet. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).  
5. ☐ Applicant's reply has overcome the following rejection(s): \_\_\_\_\_.  
6. ☐ Newly proposed or amended claim(s) \_\_\_\_\_ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).  
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.  
The status of the claim(s) is (or will be) as follows:  
Claim(s) allowed: \_\_\_\_\_.  
Claim(s) objected to: \_\_\_\_\_.  
Claim(s) rejected: 1-15.  
Claim(s) withdrawn from consideration: \_\_\_\_\_.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).  
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).  
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:  
The affidavit for reasons noted in No. 3 above.  
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). \_\_\_\_\_  
13. ☐ Other: \_\_\_\_\_

David Y. Jung  
Primary Examiner

*[Signature]*  
12/23/05

## Continuation of 3. NOTE: Response to Arguments

1. Applicant's arguments filed 30 November 2005 have been considered, but are not persuasive. With respect to 'the declarations that the actual reduction to practice was prior to Bahl's filing date of February 22, 2000 ... Consequently, all the rejections relying on Bahl should be withdrawn'. The Office does not agree for the following reasons, the declarations are deficient in showing conception or reduction in practice as well as lacking in showing diligence; in addition an affidavit or declaration is not proper to overcome a rejection if the reference is claiming essentially the same invention as the applicant. Therefore in order to correct affidavit submission, the applicant needs to show proof of conception, reduction in practice, as well as, the applicant needs to shown diligence in filing the application of the invention. If the reference and the applicant are claiming the same invention interference would be proper a declaration would not overcome the rejection.

In addition note that the applicant filing date was on 5 January 2001, and they are swearing back to some unknown date, which has been blacked out probably due to document scanning prior to 22 February 2000, which precedes the date of filing by over 10 months.

Therefore it has not been established that present invention was reduced to practice prior to February 22, 2000.

## Affidavit or Declaration Under CFR 1.131, Ineffective, Insufficient Evidence of Conception.

2. The Declaration filed on 20 November 2005 under 37 CFR 1.131 has been considered but is ineffective to overcome the Bahl et al. U.S. Patent No. 6,834,341 (hereinafter '341) reference.

3. The '341 reference is a U.S. patent or U.S. patent application publication of a pending or patented application that claims the rejected invention. An affidavit or declaration is inappropriate under 37 CFR 1.131(a) when the reference is claiming the same patentable invention, see MPEP § 2306. If the reference and this application are not commonly owned, the reference can only be overcome by establishing priority of invention through interference proceedings. See MPEP Chapter 2300 for information on initiating interference proceedings. If the reference and this application are commonly owned, the reference may be disqualified as prior art by an affidavit or declaration under 37 CFR 1.130. See MPEP § 718. Claim 1 of the applicant is claiming the same invention as claim 7, which depends from claims 1, 2, 3, and 6 of the '341 reference.

4. The evidence submitted is insufficient to establish a conception of the invention prior to the effective date of the '341 reference. While conception is the mental part of the inventive act, it must be capable of proof, such as by demonstrative evidence or by a complete disclosure to another. Conception is more than a vague idea of how to solve a problem. The requisite means themselves and their interaction must also be comprehended. See *Mergenthaler v. Scudder*, 1897 C.D. 724, 81 O.G. 1417 (D.C. Cir. 1897). The evidence submitted does not show proof that the invention was conceived prior to February 22, 2000. The applicant did not provide any legible documentation for actions prior to the filing date of application 5 January 2001.

5. The evidence submitted is insufficient to establish diligence from a date prior to the date of reduction to practice of the '341 reference to either a constructive reduction to practice or an actual reduction to practice. Diligence is lacking because no documents were submitted that show applicant or legal representatives were actively working on the invention. An example of proof would be communication between themselves and an attorney for drafting the application. The exhibit shown does not provide any visible date it was submitted, or any diligence for the ten months required to file the application.

6. The oath or declaration is defective. A new declaration in compliance with 37 CFR 1.67(a) identifying this application-by-application number and filing date is required. See MPEP §§ 602.01 and 602.02.

***DETAILED ACTION***

1. This action is responsive to communication: 2 May 2005 with original application filed on 05 January 2001 and acknowledgement of priority established by affidavit to 01 December 2000.

2. Claims 1-15 are currently pending in this application. Claims 1, 7, and 10 are independent claims.

***Response to Arguments***

3. Applicant's arguments with respect to claims 1-15 have been considered but are moot in view of the new ground(s) of rejection. The Final Rejection of 28 February 2005 is replaced with this Final Office action of October 2005. The finality of this rejection is due to the amendment of the independent claims on 01 September 2004, which necessitated the new rejection as well as the affidavit submitted 2 May 2005.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

5. Claims 1-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Bahl et al. U.S. Patent No. 6,834,341 (hereinafter '341).

Art Unit: 2134

As to independent claim 1, **"A wired network for providing secure, authenticated access to wireless network clients, comprising: a server connected to a wireless network access point, and having access to the wired network, the server being operative to perform authentication for a wireless client establishing a connection to the server through the wireless network access point"** is taught in '341 col. 2, line 57 through col. 3, line 25;

**"the server performing authentication by examining authentication information transmitted from the client to the server and determining whether or not the authentication information identifies the wireless network client as authorized to gain access to the wired network"** is disclosed in '341 col. 12, line 24 through col. 13, line 25;

**the server being operative to establish a connection session upon authentication of a client, the server being also operative to provide the client with a wired network address valid for the connection session upon authentication of the client"** is taught in '341 col. 11, lines 35-45;

**"the server being further operative to encrypt communications with the wireless network access point, the server being further operative to provide a cryptographic key valid for the connection session to the client upon authentication of the client"** is shown in '341 col. 13, lines 34-66;

**"and a user database accessible to the server for use in validating wireless clients"** is disclosed in '341 col. 12, lines 50-67.

As to dependent claim 2, **"also including a network hub providing connections between the server and additional resources on the wired network"** is shown in 'col. 8, lines 41-67.

Art Unit: 2134

As to dependent 3, “also including a router providing connections between the server and additional resources on the wired network as well as a connection to an additional wired network” is disclosed in ‘341 col. 8, lines 41-67.

As to dependent 4, “wherein the server is operative to provide addresses to clients through dynamic host control protocol” is taught in ‘341 col. 6, line 66 through col. 7, line 3 and col. 11, lines 35-45.

As to dependent 5, “wherein the server is operative to communicate with a wireless network client using point to point tunneling protocol” is shown in ‘341 col. 9, lines 44-50.

As to dependent 6, “wherein the server employs 128-bit crypto-processing to communicate with the wireless network client” is disclosed in ‘341 col. 14, lines 23-28.

As to independent 7, “A wireless network for providing secure authenticated communication between clients of the wireless network and a wired network, comprising: a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network the wireless network access point being operative to conduct communications with the server in order to authenticate wireless network clients as authorized to access the wired network” is taught in ‘341 col. 2, line 57 through col. 3, line 25;

“the wireless network access point being further operative to receive authentication information from one or more wireless network clients” is shown in ‘341 col. 9, lines 33-50;

“and transfer the authentication information to the server in order to allow the server to examine the authentication information for a wireless network client and

Art Unit: 2134

determine if the information indicates that the wireless network client is authorized to access the wired network” is shown in ‘341 col. 10, lines 26-36;

“the wireless network access point being operative to receive a cryptoprocessing key from the server upon authentication of a client and to transfer the key to that client” is disclosed in ‘341 col. 13, lines 65-66;

“and a plurality of wireless network clients operative to establish connections with the wireless network access point, each client being operative to conduct encrypted communications with the server through the access point, to pass authentication information to the network access point in order to indicate to a server communicating with the wireless network and a wired network” is shown in ‘341 col. 12, lines 34-67;

“whether or not the wireless client is authorized to gain access to the wired network, each wireless network client being further operative to and receive address information and crypto-processing data from the network access point upon authentication by the server in order to allow communication with the wired network” is disclosed in ‘341 col. 11, lines 35-45 and col. 6, line 66 though col. 7, line 3;

“each client being operative to conduct encrypted transfer of data to and from the wired network through the access point upon receiving the address and cryptoprocessing information” is taught in ‘341 col. 14, lines 2-9.

As to dependent 8, “wherein the access point communicates with the server using point to point tunneling protocol” is shown in ‘341 col. 9, lines 44-50.

As to dependent 9, “including a hub connecting the wireless network access point and a plurality of additional network access points, each additional network access point

Art Unit: 2134

communicating with a plurality of additional wireless network clients, the wireless network access point and- the additional network access points being operative to establish connections with the server through the network hub” is disclosed in col. 9, line 33 through col. 10, line 10.

As to independent 10, “A method of secure communication between wireless network clients and a wired network, comprising the steps of: establishing a connection between a wireless network access point and a security base (SB) server connected to the wired network; establishing a connection between the SB server and a wireless network client communicating with the SB server through the wireless network access point” is taught in ‘341 col. 2, line 57 through col. 3, line 25;

“exchanging encryption keys between the SB server and the wireless network client” is disclosed in ‘341 col. 13, line 65-66;

“transmitting authentication information from the wireless network client to the SB server through the wireless network access point; performing authentication for the wireless network client by examining the authentication information to determine if the wireless network client is authorized to gain access to the wired network” is taught in ‘341 col. 12, line 24 through col. 13, line 25;

“if authentication fails, rejecting connection to the wired network” is shown in ‘341 col. 7, lines 1-3;

“and if authentication passes, accepting connection to the wired network, providing a temporary wired network address” is disclosed in ‘341 col. 11, lines 35-45;



**“and a unique session encryption key to the wireless network client”** is taught in ‘342 col. 13, lines 36-40;

**“and providing access to wired network resources in response to requests by the wireless network client”** is shown in ‘col. 8, lines 41-67.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘341 as applied to claim 10 in further view of Massarani U.S. Patent No. 6,393,484 (hereinafter ‘484).

As to dependent claim 11, **“and wherein the step of accepting the connection is accompanied by a step of logging the acceptance”** is taught in ‘341 col. 18, lines 33-51 **“The PANS serve 302 keeps track of the number of bits that are transmitted by the user and sees that the user is billed accordingly”**;

the following is not taught in ‘341 **“wherein the step of rejecting connection to the wired network is accompanied by a step of logging the rejection”** however ‘484 teaches **“If the MAC address is not registered, the DHCP server refuses to handle the request, logs the attempt, potentially alerting network operators of a security breach”** in col. 3, lines 33-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access as well as an authentication/negotiation component with service providers taught in '341 to include a means to log rejections. One of ordinary skill in the art would have been motivated to perform such a modification to prevent unauthorized visitors see '484 (col. 1, lines 14 et seq.). "With the vast increase of private, semi-public and public shared-medium IP networks, a growing problem for network and service administrators is how to control and restrict access to the networks only to authorized and registered devices and users. One example of the problem relates to corporate IP network administrators who deal with an increasingly mobile work force that have deployed IP network access ports (typically IEEE 802.X or similar medium) throughout their corporate facilities for shared use by their corporate employees. Such shared network access ports work in conjunction with Dynamic Host Control Protocol (DHCP) servers to dynamically assign the appropriate IP address and other parameters to a mobile employee's device. A strong concern in the use of such networks is preventing visitors or unauthorized persons from taking advantage of the exposed network access ports to gain IP connectivity to the internal corporate network (intranet)".

As to dependent 12, "wherein the step of providing a temporary wired network address to the wireless network client includes using dynamic host control protocol to provide the address" is shown in '341 col. 6, line 66 through col. 7, line 3 and col. 11, lines 35-45 "For example, an IP address might be temporarily granted to a user via a DHCP or NAT process" and "The authentication/negotiation component 110a can also include (although it is not specifically shown) a dynamic host configuration protocol (DHCP) server that is responsible for

Art Unit: 2134

issuing and managing IP addresses. DHCP servers are known and will not be further discussed herein”.

As to dependent 13, “wherein communication between the wireless network client and the wired network server is performed using point to point tunneling protocol” is shown in ‘341 col. 9, lines 44-50 “The client can comprise any suitable computing device which, in this example, is configured for wireless communication. Each of the wireless nodes is connected through an access module 112a. In the wireless example, each access module 112a comprises one or more access points 306 that permit wireless access in known ways using known protocols”.

8. Claims 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘341 in further view of 484 in further view of Schuster et al. U.S. Patent No. 6,857,072 (hereinafter ‘072).

As to dependent 14, “wherein the step of performing authentication for the wireless network client includes transferring authentication information between the wireless network client and the SB server and wherein the authentication information is encrypted” is taught in ‘341 col. 12, lines 62-64 “One example of a secure link can be one that is established through the use of Secure Socket Layer (SSL) techniques. By authenticating the user in this manner, the user's authentication information is encrypted before it leaves the client machine”;

the following is not taught in the ‘341 and ‘484 combination:

**“using public key cryptography”** however ‘072 teaches **“One advantage of the PID-Enabled Data Network Telephony System 100 in FIG. 1 is that it may be used to provide encryption and/or authentication services. In one embodiment, the PID 110 is able to determine and exchange encryption and/or authentication data, such as a public encryption and/or authentication keys ... over a privacy network”** in col. 6, lines 44-64.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access as well as an authentication/negotiation component with service providers that also tracks rejections taught in the combination of ‘341 and ‘484 to include a means to utilize a public/private key encryption mechanism. One of ordinary skill in the art would have been motivated to perform such a modification so that sensitive data may be transmitted more securely see ‘072 (col. 3, lines 30 et seq.). **“The present invention addresses the above needs by providing a system in a data network telephony system, such as for example, the Internet, that enables encryption and/or authentication on the telephony system. Users may participate in transactions with each other using more secure data channels. Sensitive data may be transmitted more safely across public networks”**

**As to dependent 15, “wherein the step of providing a unique session encryption key includes encrypting the unique session encryption key”** is taught in ‘341 col. 13, lines 36-40 **“step 414 generates a unique token for the user. In the illustrated and described example, the PANS server 302 generates a unique token or key for each of the individual users. Step 416 then provides the user token or key to client machine for use during the user's session. Specifically, the token or key is used by the client computer each time a data packet is sent to the Internet via**

Art Unit: 2134

the PANS server 302 ... As a further added degree of security, each token or key that is used by a particular user is encrypted so that unscrupulous users cannot steal another user's token. In this example, only the client computer and the PANS server know the particular user's token or key. Any suitable encryption techniques can be used to encrypt the user's token";

"using public key cryptography" is shown in '072 col. 6, lines 44-64.

### **Conclusion**

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran  
Patent Examiner  
Technology Center 2134  
06 October 2005



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100